COSMOS
Navigate the Compliance Universe

Compliance Today - April 2018
Business associates: Have you really integrated them into your risk profile?

By Marti Arvin

Marti Arvin (marti.arvin@cynergistek.com) is Vice President of Audit Strategy at CynergisTek in Austin, TX.

When the HIPAA Privacy Rule became enforceable in April of 2003, many organizations made efforts to assure a business associate agreement (BAA) was in place when a vendor was clearly going to handle protected health information (PHI). However, the level of effort was quite varied. Since that time, organizations have increased and improved on these efforts. With the changes under the HITECH Act[1] and the corresponding implementing regulations, organizations updated their agreements and made efforts to get newly signed BAAs with current vendors by the September 23, 2014 deadline.

In April of 2012, the Office for Civil Rights (OCR) entered the first Resolution Agreement and Corrective Action Plan (RA/CAP) that involved a finding regarding the lack of a BAA.[2] Still, many organizations did not give this significant attention until OCR began its Phase II audit process in the beginning of 2016. One of the initial steps of that process asked covered entities to provide a list of their business associates. This request had some covered entities scrambling to produce the list and questioning the completeness of their list. Later in 2016, OCR had its first RA/CAP that involved the failure to update a BAA in a timely manner.[3] The resolution amount was $400,000. Almost exactly six months later, another agreement was entered with OCR over the failure to obtain a BAA.[4] This time the amount was only $31,000.

All of this demonstrates the regulatory obligation to assure that when a covered entity engages a vendor to perform a service for or on its behalf and the vendor will create, receive, maintain, or transmit PHI in the performance of said activities, the covered entity will obtain satisfactory assurance that the business associate will appropriately safeguard the information.[5] These assurances are obtained through a BAA. However, obtaining a BAA that meets the regulatory provisions may not be sufficient to appropriately address risks.

Implications to the covered entity's risk profile

Although an organization might be doing a good job of getting a BAA in place, that is not enough to fully address the risk a business associate relationship may pose to the covered entity. This is not a one-and-done undertaking. The assessment of how the business associate fits in to the covered entity's risk profile is an ongoing process throughout the life cycle of the relationship. It starts with the due diligence necessary prior to beginning the relationship and goes through the processes needed to end the relationship. Questioning the business associate's compliance during this entire process is necessary to accomplish this.

The regulations require the covered entity to obtain satisfactory assurances through the BAA, but there is no guarantee the business associate will appropriately safeguard the information. Further, other than the mandated provisions of a BAA, there is no definition in the regulations that clarifies what the "satisfactory assurances" must be. OCR has clarified through its FAQ process that a covered entity is not obligated to monitor how a business associate specifically is safeguarding the covered entity's data. However, failure to perform any due

diligence can create risks for the covered entity. Let's look at one example to demonstrate this — a data compromise at the business associate.

Under the HIPAA Security Rule, a BAA must include a provision requiring the business associate to notify the covered entity of any security incidents.[6] The rule defines a security incident as "the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with systems operations in an information system."[7]

Most organizations have dozens if not hundreds of business associates. Although all of the vendors who fit the definition of a business associate might not have large volumes of an organization's PHI, a significant percentage will. Most organizations I speak with have had very few notifications from their business associates of a security incident. In that same vein, I have encountered very few organizations that believe their business associates are not being impacted by the same cybersecurity issues as others in the healthcare space.